JAVNO NAROČILO: »Vzdrževanje strojne in sistemske programske opreme«

TEHNIČNE SPECIFIKACIJE IN ZAHTEVE

Uvod

Namen dokumenta

Namen dokumenta je pregled tehničnih specifikacij za strojno, programsko, sistemsko in komunikacijsko opremo ter predstavitev sistema, vzdrževanja in nadgradnje:

- sistemske infrastrukture Univerze v Ljubljani, Medicinske fakultete,
- ocene stroškov in terminskega načrta izvajanja del za vzdrževanje, nadgradnjo ter druga opravila.

Dokument opisuje lastnosti sistemske infrastrukture Univerze v Ljubljani, Medicinske fakultete.

Univerza v Ljubljani, Medicinska fakulteta (naročnik) z dokumentom opredeljuje cilje, ki jih želi doseči z informacijsko rešitvijo. Dokument je del razpisne dokumentacije za izbor izvajalca, ki bo odgovoren za vzdrževanje, načrtovanje, razvoj ter uvedbo rešitve in zagotavljanje delovanja infrastrukture. Dokument morajo obvezno prebrati:

- člani IT skupine Univerze v Ljubljani, Medicinske fakultete,
- načrtovalci modularnih in sistemskih testiranj,
- sistemski in aplikacijski skrbniki (administratorji),
- ponudniki informacijskih storitev.

Dokument ponudnikom omogoča razumevanje naročnikovih zahtev ter oceno predvidenega obsega del na podlagi drugih predpostavk in pogojev v razpisni dokumentaciji. Na podlagi teh specifikacij in sistemske analize bo v sodelovanju z naročnikom izdelan prototip informacijskega sistema. Dokument priporočamo v branje:

- vodjem IKT rešitev in projektov,
- vodjem razvoja IKT rešitev,
- skrbnikom ključnih strank,
- izvajalcem izobraževanj.

Obseg produkta

Obseg predstavlja tekoče vzdrževanje in upravljanje IT storitve, ki jo delimo na:

- vzdrževanje ravni IT storitve (ohranjanje delujočega stanja);
- preventivno vzdrževanje (nadzor rešitve, posodabljanje, redni pregledi, testiranje redundanc…);
- redno administriranje IT storitev uporabnikov (spreminjanje in upravljanje, …);
- nadgradnje IT storitev;
- vzdrževanje vseh nadgradenj;
- reševanje incidentov;
- upravljanje IT storitve:
- nadzor izvajanja IT storitve;
- vodenje evidenc in poročanje.
- Nudenj DRC storitve za posamezna področja.

Predmet javnega naročila je:

- Osnovno in dopolnilno vzdrževanje strežniške strojne in sistemske programske opreme.
- Osnovno in dopolnilno vzdrževanje omrežja.
- Vzpostavitev oziroma nadgradnja sistema za nadzor sistemske infrastrukture.
- Nudenje DRC storitve.
- Ustrezne licence za zagotavljanje podpore mrežne opreme (podrobnosti so navedene v dokumentaciji).

Definicije, akronimi in kratice

Definicije

IT rešitev je skupek strojne in programske opreme, ki zagotavljanje informacijsko podporo poslovnim procesom (v besedilu se smiselno uporablja tudi beseda rešitev).
IT storitev (v besedilu se smiselno uporablja tudi beseda storitev) je IT rešitev skupaj s storitvami upravljanja.

Kratice

CSV	Comma-separated Values (z vejico ločeni podatki)
API	Application Programming Interface (Aplikacijski programski vmesnik)
GDPR	Splošna uredba o varstvu podatkov
DRC	Disaster Recovery Center (lokacija, ki začasno služi za delovanje informacijskega sistema v primeru katastrofe)
PDF	Portable Document Format
SSO	Single Sign On (Enkratna prijava uporabnika)
TLS	Transport Layer Security
MFA	Multi-Factor Authentication (več stopenjsko overjanje)
UL MF	Univerza v Ljubljani, Medicinska fakulteta
IMI	Inštitut za mikrobiologijo in imunologijo
IP	Inštitut za patologijo
ISM	Inštitut za sodno medicino
VPN	Navidezno zasebno omrežje

Opis sistemske infrastrukture

Namen sistemske infrastrukture

Sistemska infrastruktura Medicinske fakultete Univerze v Ljubljani je namenjena zagotavljanju stabilnega, varnega in učinkovitega delovanja informacijskih sistemov, ki podpirajo:

Pedagoški proces – dostop do učnih virov, e-učilnic, akademskih baz podatkov in komunikacijskih platform.

Raziskovalno dejavnost – obdelavo znanstvenih in shranjevanje raziskovalnih podatkov.

Administrativno poslovanje – upravljanje študentskih in kadrovskih podatkov, računovodskih sistemov ter dokumentacijskih tokov.

Zdravstveno dejavnost – integracijo s kliničnimi informacijskimi sistemi, podporo laboratorijem in diagnostičnim enotam.

Kibernetsko varnost – zaščito občutljivih podatkov in zagotavljanje skladnosti z zakonodajnimi zahtevami (GDPR, SUVI).

Sestava sistemske infrastrukture

Strežniška infrastruktura

Več fizičnih in virtualnih strežnikov v VMware okolju.

Diskovna polja z visoko razpoložljivostjo in redundantnim sistemom shranjevanja podatkov.

Varnostne kopije na platformi Veeam, ki zajemajo več kot 300 virtualnih strežnikov.

Mrežna infrastruktura

Omrežje temelji na opremi proizvajalcev Cisco in HP, obsega vsaj 250 omrežnih naprav.

Upravljanje varnostnih kopij in omrežnega prometa prek centraliziranega nadzora.

Mrežna infrastruktura Medicinske fakultete UL zagotavlja zanesljivo, varno in hitro povezljivost za vse uporabnike. Omrežje je sestavljeno iz naslednjih glavnih komponent:

- Hrbtenično (core) omrežje – centralna hrbtenica omrežja, ki povezuje vse glavne stavbe in podatkovne centre fakultete.
- Dostopovna plast (access layer) – zagotavlja povezljivost za uporabniške naprave, kot so računalniki, tiskalniki in raziskovalna oprema.
- Brezžično omrežje (Wi-Fi) – dostopna točka za zaposlene, študente in goste s podporo za varnostne protokole WPA2-Enterprise.
- Varnostne komponente – vključujejo požarne pregrade (firewall), sistem za preprečevanje vdorov (IPS) in IDS na Inštitutu za Patologijo in Inštitutu za mikrobiologijo in imunologijo.
- Oddaljeni dostop (VPN) – omogoča varno povezavo do fakultetnega omrežja za zaposlene in raziskovalce ter zunanje sodelavce.

Uporabniška oprema

Več kot tisoč petsto delovnih postaj za zaposlene in študente.

Sistemi za skupno in varno tiskanje (Inštitut za patologijo - velja za sklop 2).

VPN in oddaljeni dostopi za raziskovalce in administrativno osebje.

Podatkovni center DRC

Rešitev za obnovo podatkov v primeru katastrofe (Disaster Recovery Center) samo za Inštitut za patologijo - velja za sklop 2.

Sistemska infrastruktura pokriva več lokacij UL MF, vključno z glavno stavbo, Inštitutom za patologijo, Inštitutom za mikrobiologijo in imunologijo ter Inštitutom za sodno medicino.

Sistemska infrastruktura UL MF je razdeljena na centralno infrastrukturo, ki jo uporabljajo vsi uporabniki UL MF, vključno z Inštitutom za patologijo, Inštitutom za mikrobiologijo in Inštitutom za sodno medicino, ter na zaključene samostojne enote teh inštitutov za katere se uporabljajo samostojni gradniki.

Rezervno opremo priskrbi izvajalec preko garancije ali iz zaloge naročnika, če oprema ni v garanciji.

Časi prijave okvare in pristopa k okvari za opremo HPE (Hewlett Packard Entreprise) morajo biti zagotovljeni s podporo proizvajalca v režimu Next Business Day (5x9/NBD) s časom prijave okvare v delovnikih med 8:00 in 17:00.

Stroške, povezane z nakupom licenc, v celoti krije naročnik. Velja za vse sklope javnega naročila.

Garancijo za opremo krije naročnik. Izvajalec mora naročnika pravočasno obvestiti o poteku garancije ter predlagati eno izmed naslednjih možnosti: podaljšanje garancije, nakup nove opreme ali alternativno rešitev. Ta določba velja za vse sklope javnega naročila.

Centralna računalniško in komunikacijska infrastruktura UL MF (velja za sklop 1)

Centralna računalniško in komunikacijska infrastruktura UL MF je osnovni okvir, ki omogoča delovanje informacijskega sistema organizacije UL MF. Sestavljena je iz strojnih, programskih in komunikacijskih komponent, ki skupaj zagotavljajo nemoteno delovanje računalniških omrežij, strežnikov, shranjevanja podatkov, komunikacijskih sistemov in drugih ključnih elementov, potrebnih za podporo poslovanja organizacije.

Centralna infrastruktura omogoča povezavo v omrežja Arnes, Metulj in zNet ter zagotavlja povezavo z internetom. Poskrbi za povezljivost vseh oddaljenih enot v skupno omrežje ter omogoča povezavo z DRC (le za Inštitut za patologijo). V centralno infrastrukturo so povezane naslednje lokacije:

Vzdrževanje strojne in sistemske opreme se izvaja na lokacijah Univerza v Ljubljani, Medicinska fakulteta, predvsem na naslednjih naslovih:

- Vrazov trg 1, Ljubljana
- Vrazov trg 2, Ljubljana
- Korytkova 2, Ljubljana
- Korytkova 2a, Ljubljana
- Zaloška 2, Ljubljana
- Zaloška 4, Ljubljana
- Zaloška 7, Ljubljana
- Zaloška 7 a, Ljubljana
- Zaloška 9, Ljubljana
- Zemljemerska 12, Ljubljana
- Grablovičeva ulica 46, Ljubljana
- Japljeva 2, Ljubljana
- Šlajmarjeva 3, Ljubljana
- Bohoričeva 20, Ljubljana
- Poljanski nasip 58, Ljubljana
- Studenec 48, Ljubljana
- Hrvatski trg 6, Ljubljana
- Linhartova 51, Ljubljana
- Dolenjska c. 29, Ljubljana
- Dolenjska cesta 242, Ljubljana
- Vodnikova cesta 62, Ljubljana
- Wolfova 12, Ljubljana

Lokacije se lahko spreminjajo zaradi selitev, saj so nekatere stavbe Medicinske fakultete trenutno v fazi prenove ali novogradnje.
Povezavi v omrežji Metulj in Arnes sta opremljeni z osrednjo požarno pregrado, dvema hrbteničnima vozliščema, zgrajenima s skladovnimi stikali, ter dvema vozliščema za povezavo osrednjih strežnikov. Omrežje vključuje razvejano optično infrastrukturo. Ključne naprave so večinoma podvojene in fizično nameščene na dveh lokacijah (na Vrazovem trgu 2 – VT2 in na Korytkovi 2 – KOR). Hrbtenični vozlišči povezujejo dostoptovna stikala po enotah MF (približno 50 enot), ki so locirane večinoma v stavbah na območju s premerom okoli 1 km. Vse povezave med stavbami potekajo po optičnih vodnikih. Usmerjanje, funkcije IPS in druge varnostne funkcije se izvajajo na osrednji požarni pregradi v kombinaciji s centralnim upravljalnim sistemom proizvajalca Cisco.

Med ostalimi uporabljanimi protokoli so še: 802.1q, VTP V3, DHCP relaying, OSPF, QoS, BGP, VPN ter SNMP V2 in V3. Osrednje brezžično omrežje na UL MF sestavlja virtualni krmilnik in več kot 100 dostopnih točk, nameščenih v predavalnicah in drugih prostorih MF. Strežniki, diskovna polja in stikala SAN so locirani na dveh lokacijah (VT2 in KOR).

Osrednjo strežniško infrastrukturo na UL MF sestavlja 8 strežnikov, opremljenih s programsko opremo za virtualizacijo VMware. Na tej osnovi teče več deset virtualnih strežnikov z operacijskimi sistemi Windows in Linux (različne verzije). Za izdelavo rezervnih kopij podatkov se uporablja programska oprema Veeam na ločenem fizičnem strežniku, ki je povezan tudi s tračno enoto.

Na MF UL za naloge in vzdrževanje strežniške ter mrežne opreme skrbijo tri osebi. Njune naloge vključujejo osnovno sistemsko administracijo, nadzor delovanja strežnikov in omrežja, odpravljanje pogostih težav, spremljanje statusov strojne opreme, osnovno posodabljanje programske opreme ter osnovno uporabniško podporo v povezavi z delovanjem računalniške opreme. Ponudnik bo zagotovil razpoložljivost za zahtevnejše posege, svetovanje, nadgradnje ter odzivnost v primeru incidentov, vse v skladu z razpisnimi pogoji in SLA zahtevami.

Seznam mrežne opreme, ki je predmet vzdrževanja:

Kategorija	Podrobnosti	Opombe
Požarne pregrade	1 x Cisco Secure Firewall 3110 NGFW Appliance, vključno s Cisco Intrusion Prevention System (IPS), FirePower Management Center (FMC) ter s funkcionalnima licencama Thread Defense (TD) in Advanced Malware Protection (AMP) ter pripadajoči strežniki za upravljanje	V garanciji do decembra 2027, 8×7/NBD
Stikala v hrbtenici omrežja: Proizvajalec Cisco s pripadajočo sistemsko programsko opremo		
Sklad core stikal v podatkovnem centru VT2	2x WS-C3850-24XU-L, 1 x WS-C3850-12XS-S	
Sklad core stikal v podatkovnem centru KOR	2x WS-C3850-24XU-L, 2x WS-C3850-12XS-S	
Povezovalna stikala na internet	4x WS-C3750X-24T-S	
Dostopovna stikala: Proizvajalec Cisco s pripadajočo sistemsko programsko opremo		
Modeli dostopovnih stikal	18× C9200-48P 8× C9200-48T 3× C9200-48PL 6× C9200-24P 1× C9200-24T 4× C1000-8P-2G-L 3× WS-C2960X-24PS-L 3× WS-C2960X-24TS-L 1× WS-C2960X-48FPS-L 1× WS-C2960X-48TS-L 40× 24-portno stikalo serije WS-C2960 / S / Plus / G; 7× 48-portno stikalo serije WS-C2960S / Plus 1× WS-C2950G-24-EI 1× WS-C2950G-48-EI 2× WS-C2970G-24T-E	Del stikal serije C9200 je v garanciji
Dostopovne točke: Proizvajalec: Cisco s pripadajočo sistemsko programsko opremo		
Modeli dostopovnih točk	15× C9115AXI-E (vse v garanciji do avgusta 2027, NBD); 62× AIR-AP1832I-E-K9 (od tega 30x v garanciji do maja 2027, NBD); 32× AIR-CAP1702I-E-K9 5x C9115AXI-E (vse v garanciji do avgusta 2027, NBD) 5x AIR-AP1832I-E-K9 (vse v garanciji do avgusta 2025, NBD)	
Virtualni krmilnik brezžičnega omrežja	Cisco (vWLC) (opisan pod programsko opremo)	

Seznam kritične/ključne omrežne opreme (od zgoraj navedene):

sistem požarnih pregrad Cisco,

stikala v hrbtenici omrežja proizvajalca Cisco.

Seznam strežniške opreme, ki je predmet vzdrževanja:

Kategorija	Podrobnosti	Opombe
Strežniki	8 x strežnik za podporo VMWare 2 x za backup Lenovo ThinkSystem SR650, 1x HPE DL 380 GEN8, 2x HPE DL 380 GEN9, 2x HPE DL 380 GEN10 in 1x Dell PowerEdge R740 (v garanciji do avgusta 2025); 2 x diskovni polji: Lenovo in HPE; 4 x stikala SAN HPE; 1 x tračna enota HPE MSL2024; 1 x ExaGrid EX18 - Disk Capacity: Raw: 48 TB, Useable : 36 TB. - 18 TB Full Backup	Lenovo ThinkSystem SR650 (v garanciji do februarja 2027, 6CTR) Diskovno polje, Lenovo ThinkSystem DE6000E (v garanciji do avgusta 2028, 6CTR) ExaGrid EX18 : Garancija - 5 letna podpora in vzdrževanje

Seznam kritične/ključne strežniške opreme (od zgoraj navedene):

2x, strežnik, Lenovo ThinkSystem SR650 (v garanciji do februarja 2027, 6CTR);

2x, strežnik, HPE ProLiant DL380 Gen10;

1x, diskovno polje, Lenovo ThinkSystem DE6000E (v garanciji do avgusta 2028, 6CTR);

1x, diskovno polje, HPE MSA 2052 SAN DUAL CTRL SFF;

4x, SAN stikalo, HPE SN3000B 16GB 24-PORT/12.

Seznam programske opreme, ki je predmet vzdrževanja:

Kategorija	Podrobnosti
Strežniki	2 x VMWare Essentials Plus, 1x VMWare Essentials; 1 x Veeam Backup Essentials Enterprise; 1 x Virtual Wireless LAN Controller Cisco WLC-9800-CL (vWLC virtualni krmilnik brezžičnega omrežja Cisco; v garanciji do avgusta 2025); 1 x Ipswitch WhatsUp Gold (WUG) MSP Edition Remote (programska oprema za nadzor delovanja računalniške opreme; deluje v povezavi z operatersko licenco WhatsUp Gold - to licenco zagotavlja izvajalec, licenca velja do 17. 5. 2026); 1 x SolarWinds Kiwi CatTools (programska oprema za izdelavo rezervnih kopij konfiguracij opreme); 30 x Windows strežniški operacijski sistemi(različne verzije); 40 x Linux strežniški operacijski sistemi (različne odprtokodne verzije);

Seznam kritične/ključne programske opreme (od zgoraj navedene):

2 (dva) VMWare Essentials Plus;

14 ključnih strežnikov z Linux operacijskim sistemom (storitve na njih so v grobem razvidne iz imena strežnika): MAIL-mbs2, MAIL_avs4, MAIL_mailman2, MAIL_webmail2, MF_www, MF_www_hosting2,

NET_idp-produkcija, NET_ldap-slave1-new, NET_net1, NET_net2, NET_posta, NET_radius1, NET_radius2, NET_rls-new;

6 ključnih strežnikov z Windows operacijskim sistemom: MEF_dcv1mf_2022, MEF_dcv2mf_2022, MEF_fsv3mf, MF_RemoteAppSrv, IPTEL_DLS_server, NET_WinSRV_veeam2.

Oprema je razporejena med lokacijama.

Izvajalec mora zagotavljati pripravo in ustrezno delovanje mrežne opreme in strežniških sistemov (fizičnih in/ali virtualnih), ki delujejo na platformi, ki jo ima naročnik v lasti. Strežniška infrastruktura zajema:

- fizični strežniki,
- virtualni strežniki na virtualni infrastrukturi ,
- diskovne kapacitete na strežniških sistemih (fizičnih ali virtualnih) s pomočjo diskovnega podsistema;
- omrežje SAN.

Izvajalec bo moral, v dogovoru z naročnikom, ostalim ponudnikom omogočati uporabo mrežne opreme, strežniške infrastrukture.

Računalniško in komunikacijska infrastruktura Inštituta za patologijo (velja za sklop 2)

Računalniško in komunikacijska infrastruktura za patologijo zagotavlja podporo procesom na področju patologije za zagotavljanje najsodobnejše diagnostike ter uspešno raziskovalno in pedagoško delo. Infrastrukturo sestavljajo mrežna oprema, strežniki, virtualno okolje, varnostni sistemi ter podatkovni center za obnovo (DRC). Pri izmenjavi podatkov z zunanjimi sistemi se uporablja centralna računalniško in komunikacijska infrastruktura UL MF.

Na IP za naloge in vzdrževanje strežniške ter mrežne opreme, kakor tudi za osebne računalnike, skrbijo tri osebe. Njihove naloge vključujejo osnovno sistemsko administracijo, nadzor delovanja strežnikov in omrežja ter varnostnih kopij (DPM, Veeam), odpravljanje pogostih težav, spremljanje statusov strojne opreme, posodabljanje programske opreme ter osnovno uporabniško podporo v povezavi z delovanjem računalniške opreme. Ponudnik bo zagotovil razpoložljivost za zahtevnejše posege, svetovanje, nadgradnje ter odzivnost v primeru incidentov, vse v skladu z razpisnimi pogoji in SLA zahtevami.

Seznam mrežne opreme, ki je predmet vzdrževanja:

Kategorija	Podrobnosti
Mrežne naprave:	2 x Cisco core stikali Catalyst 3850 2x Cisco core stikali Nexus 9300 11 x Cisco access stikala
Požarne pregrade:	2 x Fortinet požarna pregrada FG-101F 2x NginxWAF

Seznam kritične/ključne mrežne opreme:

2 x Cisco core stikali
11 x Cisco access stikala
2 x Fortinet poiarna pregrada
2x NginxWAF

Seznam strežniške opreme, ki je predmet vzdrževanja

Kategorija	Podrobnosti
Strežniki:	3 x DELL strežniki - hiperkonvergenčni sistem 1 x Diskovno polje Dell PowerVault ME5084 70 Virtualnih strežnikov (V kar niso zajeti VM-ji, ki so računalniki z Windows 10, torej virtualni PC-ji)

Seznam kritične/ključne strežniške opreme:
3 x DELL strežniki - hiperkonvergenčni sistem;

1 x Diskovno polje Dell PowerVault ME5084.

Seznam programske opreme, ki je predmet vzdrževanja:

Kategorija	Podrobnosti
Programska oprema	Windows server 2016 in novejši, MS Domain Services (Active Directory, GPO, DNS), MS CA, MS DFS, MS NPS, MS IIS spletni strežnik, MS Hyper-V Cluster s Storage Spaces Direct, MS Print Management, MS Remote Desktop Services license server MS Remote Desktop Gateway MS SQL Server Enterprise/Standard, MS SCCM (build računalnikov in nameščanje programske opreme), MS WSUS, AlmaLinux Fedora Linux F5 Nginx Veeam Backup&Replication, VeeamONE Zabbix monitoring infrastrukture (omrežna in strežniška infrastruktura) in aplikacij (Labex)*

*Ponudnik mora zagotoviti vzpostavitev storitev Zabbix monitoringa na način gostovanja Zabbix stražnika in se pri naročniku nahaja zgolj proxy.

Kritični/ ključni servisi:
MS Domain Services (Active Directory, GPO, DNS),
MS CA,
MS DFS,
MS NPS,
MS IIS spletni strežnik,
MS Hyper-V Cluster s Storage Spaces Direct,
MS Application virtualization,
MS Print Management,
MS SQL Server Enterprise/Standard,
F5 Nginx
Veeam Backup&Replication, VeeamONE
Zabbix monitoring infrastrukture (omrežna in strežniška infrastruktura) in aplikacij (Labex)

Spletna stran

Vzpostavitev in zagotavljanje gostovanja spletne strani z naslednjimi komponentami:

- aplikacijski strežnik,
- bazni strežnik,
- reverse proxy za objavo spletne strani v internet,
- tehnična podpora za sistem Wordpress.

Minimalne tehnične zahteve

Strežniški viri in gostovanje:

Inicialna velikost prostora za gostovanje mora znašati najmanj 10 GB,
omogočena mora biti skalabilnost infrastrukture (možnost povečanja prostora, pomnilnika ipd.),
gostovanje mora vključevati aplikacijski in bazni strežnik,
strežniki morajo biti ustrezno zavarovani.

Dostop do spletne strani:

Spletna stran mora biti objavljena v internet prek reverse proxy strežnika, ki ga zagotovi ponudnik,
reverse proxy mora omogočati ustrezne varnostne mehanizme (npr. HTTPS, zaščita pred napadi DDoS, WAF ipd.).

Razvojno in testno okolje:

Ponudnik mora vzpostaviti ločeno staging (testno) okolje za testiranje novih funkcionalnosti, omogočeno mora biti:
tehnično preverjanje sprememb s strani razvijalcev,
funkcionalno testiranje s strani naročnika,
preverjanje varnosti in stabilnosti s strani ponudnika pred prenosom v produkcijo.

Upravljanje sprememb in verzioniranje:

Ponudnik mora zagotoviti Git repozitorij, preko katerega pooblaščeni razvijalci naročnika oddajajo spremembe,
repozitorij mora biti integriran v razvojni potek z avtomatiziranim prenosom sprememb v staging okolje,
vse spremembe se najprej uveljavijo v staging okolju in šele po potrditvi vseh treh deležnikov (razvijalec, naročnik, ponudnik) prenesejo v produkcijo.

Tehnična podpora:

Ponudnik mora zagotavljati tehnično podporo za sistem Wordpress, ki vključuje:
sodelovanje pri osnovnem vzdrževanju sistema (posodobitve, varnostni popravki),
odpravo napak, povezanih z infrastrukturo gostovanja,
svetovanje pri integracijah v obstoječe rešitve naročnika.

DRC

Kategorija	Podrobnosti
Programska oprema	Windows server 2016 in novejši, MS Domain Services (Active Directory, GPO, DNS), MS DFS, MS NPS, Cisco Email Security Appliance (ESA) Obseg DRC je previden za 19 virtualnih strežnikov skupne kapacitete 8300 GB prostora, 185 GB RAM in 60 vCPU.
	Vzpostavitev dveh Veeam Gateeay virtualnih strežnikov vsak kapacitete (2vcpu, 4GB ram, 50GB disk) - Razširitev naročnikovega Veeam backup okolja z dodatnima DRC virtualnima strežnikoma. Skupna kapaciteta pripetih diskov 150TB na prvem in 16TB na drugem Veeam Gateway virtualnem strežniku.. Upoštevati v pavšalu prirastek za 25TB na leto na prvem Veeam Gateway virtualnem strežniku.

Računalniško in komunikacijska infrastruktura Inštituta za mikrobiologijo in imunologijo (velja za sklop 3)

Računalniško-komunikacijska infrastruktura za Inštituta za mikrobiologijo in imunologijo zagotavlja podporo procesom za zagotavljanje najsodobnejše diagnostike ter uspešno raziskovalno in pedagoško delo. Infrastrukturo sestavljajo mrežna oprema, strežniki, virtualno okolje, varnostni sistemi ter podatkovni center za obnovo (DRC). Pri izmenjavi podatkov z zunanjimi sistemi se uporablja centralna računalniško-komunikacijska infrastruktura UL MF.

Na IMI za naloge in vzdrževanje strežniške ter mrežne opreme, kakor tudi za osebne računalnike, skrbita dve osebi. Njune naloge vključujejo osnovno sistemsko administracijo, nadzor delovanja strežnikov in omrežja ter varnostnih kopij (DPM, Veeam, tračna enota), odpravljanje pogostih težav, spremljanje statusov strojne opreme preko sistema PRTG, posodabljanje programske opreme ter osnovno uporabniško podporo v povezavi z delovanjem računalniške opreme. Ponudnik bo zagotovil razpoložljivost za zahtevnejše posege, svetovanje, nadgradnje ter odzivnost v primeru incidentov, vse v skladu z razpisnimi pogoji in SLA zahtevami.

Seznam mrežne opreme, ki je predmet vzdrževanja:

Kategorija	Podrobnosti
Mrežne naprave:	2x stikalo hrbtenično Cisco 9500 (C9500-24Y4C, redundančni napajalnik) 6x stikalo Cisco C9200L-48PXG-2Y 4x stikalo Cisco C9200L-48T-4G 3x stikalo Cisco C9200L-48P-4X 2x stikalo Cisco C9200L.24T-4x 2x stikalo Cisco C1000-48P-4X-L 4x stikalo Cisco C1000-16T-2G-L 1x stikalo CiscoC1000-24T-4G-L 1x stikalo HP J9855A 2530-48G-2SFP+ 2x stikalo HP ProCurve 2520-8-PoE 3x stikalo HP 2520-24-PoE 1x stikalo HP 2610-24-PWR 1x stikalo HP ProCurve Switch 4204vl 1 3x stikalo HP 5406zl z moduli: 3x HP J8702A 24p Gig-T zl Module 1x HP J9534A 24p Gig-T PoE+ v2 zl Module 1x HP J9535A 20p GT PoE+/4P SFP v2 zl Mod 1x HP J9536A 20p GT PoE+/2p SFP+ v2 zl 1x HP J9538A 8p 10G-GbE SFP+ v2 zl Module 1x HP J8708A 4p 10G CX4 zl Module Redundantni napajalnik 1x WLAN krmilnik Cisco WLC 2504 21 x WLAN dostopnih točk Cisco povezanih v omrežje Eduroam z lastnim avtentikacijskim strežnikom (8x Cisco 1702I, 13x Cisco 1142) 5 x WLAN dostopnih točk Cisco 1832 povezanih z Cisco Mobility Express.
Požarne pregrade:	1x Požarna pregrada Fortinet 200F 1x Fortinet Analyzer 1x Požarna pregrada Cisco 5506

Seznam strežniške opreme, ki je predmet vzdrževanja

Kategorija	Podrobnosti	Opombe

Strežniki in ostala strojna oprema:	3x Lenovo ThinkSystem SR630 v2 2x Intel Xeon Gold 6326 16-core 16x 32GB DDR4-3200 2x 240GB SSD (RAID1) 2x Lenovo ThinkSystem SR630 v2 1x Intel Xeon Gold 5315Y 8-core 8x 32GB DDR4-3200 2x 240GB SSD (RAID1) 1x Lenovo ThinkSystem SR630 v2 1x Intel Xeon Silver 4310 12-core 1x 32GB DDR4-3200 2x 480GB SSD (RAID1) 1x Diskovno polje IBM Flashsystem 5200 9x 19,2TB SSD disk 2x SAN stikalo Lenovo ThinkSystem DB610S Gen6 _____ HP BladeSystem c7000 Enclosure BladeSystem c7000 Onboard Administrator 1x ProLiant BL460c G1 2x 2,3Ghz procesor, 32GB pomnilnik, 2x 10Gb mrežna kartica, 2x300GB SAS trdi disk 1x ProLiant BL460c G7 2x 2,4GHz 6-core procesor, 128GB pomnilnika, 2x 10Gb mrežna kartica. 2x300GB SAS trdi disk 1x ProLiant BL460c G6, 2x 2,27Ghz 4-core procesor, 128GB pomnilnika, 2x10Gb mrežna kartica, 1x 4Gb FC kartica, 2x600GB SAS trda diska 1x ProLiant BL460c Gen10, 2x 3 GHz 12-Core procesor, 256GB pomnilnika, 2x 10Gb mrežna kartica, 1x 16Gb FC kartica) 2x HP VC Flex-10 Enet Module 2x HP B-series 8/12c SAN Switch BladeSystem c-Class 10x Active Cool 200 Fan 6x BladeSystem c-Class power supply _____ Diskovno polje HP 3PAR 7200c 8x 480 GB SSD 24x 900 GB SAS 24x 1,2 TB SAS 16x 3TB NL SAS HPE ProLiant DL380p gen8, 653200-B21 2x 4core 3,5GHz procesor, 24Gb pomnilnika, 4x 300GB SAS, 4x 1,2TB SAS, Smart Array P420i krmilnik, 2x750W napajalnik HPE ProLiant DL380p gen8, 653200-B21 2x 4core 3,5GHz procesor, 24Gb pomnilnika, 8x 300GB SAS, Smart Array P420i krmilnik, 2x750W napajalnik HPE ProLiant DL380p gen8, 653200-B21 2x 4core 3,5GHz procesor, 24Gb pomnilnika, 4x 300GB SAS, Smart Array P420i krmilnik, 2x750W napajalnik HP D3700 Enclosure	6x Lenovo ThinkSystem SR630 v2 in 2x SAN stikalo Lenovo Think System so v garanciji do 20.5.2028 IBM FlashSystem 5200 je v garanciji do 26.1.2028 Izven garancisjko vzdrževanje Izven garancijsko vzdrževanje

	8x 1,2 TB SAS HP ProLiant DL380 Gen9 2x 480GB SAS in 10x 4TB SAS HP ProLiant DL380 Gen10 12x 16TB Tračna enota LTO-8 IBM FlashSystem 5035 7x 1,92TB SSD 12x 8TB NL SAS 2x Lenovo ThinkSystem SR 665 2x AMD 32 Core Processor 8x 32GB RAM 2x 240GB SSD disk 2x FC 16Gb kartica 2x 10/25Gb mrežna kartica 1x Tesla T4 grafična kartica Nvidia	Izven garancijsko vzdrževanje
Programska oprema/servisi (vsi strežniki delujejo v virtualnem okolju Vmware Vsphere 7.0 in 8.0)	45x Windows server 2012 R2 ali novejši 20x Linux server 2x MS 2022 Domain controller (ADC, DNS, DHCP) 1x Ubuntu Linux avtentikacijski server za Eduroam 1x MS System Center Configuration Manager 1x MS Exchange 2019 strežnik 1x MS Data Protection manager strežnik 6 x Vmware vsphere ESX 7 in ESX 8 2x Vsphere virtual center 8 1 x Veeam, 12.1 backup strežnik 1x MS CA strežnik 1x Sharepoint portal 2013 server 1x Xibo sistem za digitalno oglaševanje	

Kritična računalniška strojna oprema in servisi

Seznam kritične strojne opreme:

1x Požarna pregrada Fortinet 200F
1x Požarna pregrada Cisco 5506
Stikala navedena v seznamu mrežne opreme, ki je predmet vzdrževanja
Cisco WLC 2504 krmilnik
HP BladeSystem c7000 Enclosure
HP VC Flex-10 Enet Module
Active Cool 200 Fan
B-series 8/12c SAN Switch BladeSystem c-Class

Seznam kritičnih servisov:

2x MS 2022 Domain controller (DC, DNS, DHCP)
2x VMWARE strežniška gruča
MS Windows Server 2022 Podatkovni strežnik
Diagnostična avtomatizirana linija BD KIESTRA TLA
2x Veeam Backup

Računalniško in komunikacijska infrastruktura Inštituta za sodno medicino (velja za sklop 4)

Računalniško-komunikacijska infrastruktura za Inštituta za sodno medicino zagotavlja podporo procesom za zagotavljanje najsodobnejše diagnostike ter uspešno raziskovalno in pedagoško delo. Infrastrukturo sestavljajo mrežna oprema, strežniki, virtualno okolje, varnostni sistemi. Pri izmenjavi podatkov z zunanjimi sistemi se uporablja centralna računalniško-komunikacijska infrastruktura UL MF.

Na ISM za naloge in vzdrževanje strežniške ter mrežne opreme opravlja oseba, ki koordinira delo z zunanjim pogodbenim izvajalcev in bo predvidoma tudi v okviru tega javnega naročila. Izvajalec bo skrbel za celotno vzdrževanje sistemskega dela IKT, naročnik bo pokrival vzdrževanje aplikacij, ki so vključena in izobraževalnega dela in uporabe aplikacij UL MF. Ponudnik bo zagotovil tudi razpoložljivost za zahtevnejše posege, svetovanje, nadgradnje ter odzivnost v primeru incidentov, vse v skladu z razpisnimi pogoji in SLA zahtevami.

Seznam mrežne opreme, ki je predmet vzdrževanja:

Kategorija	Podrobnosti	Opombe
Mrežne naprave:	Uporabljajo se mrežne naprave sklopa 1	
Požarne pregrade:	1x Požarna pregrada Cisco CSF1220CX	TAMC licenca je veljavna 3 leta

Seznam strežniške opreme, ki je predmet vzdrževanja

Kategorija	Podrobnosti	Opombe
Strežniki in ostala strojna oprema:	Virtualizacijski strežnik LENOVO ThinkSystem SR650 V2 2x Intel(R) Xeon(R) Silver 4310 CPU @ 2.10GHz 128GB RAM 2x 480GB SSD 6x 3.8TB SSD Broadcom 57414 10/25GbE SFP28 2-port Redundantna napajalnika Backup strežnik Lenovo ThinkSystem SR650 V2 Intel(R) Xeon(R) Gold 5317 CPU @ 3.00GHz 16GB RAM 2x 480GB SSD 6x 12TB NL SAS Broadcom 57414 10/25GbE SFP28 2-port Redundatna napajalnika Tračna enota HE LTO-8	Virtualizacijski strežnik Lenovo ThinkSystem SR650 V2 je v garanciji do 27.8.2026 Backuo strežnik Lenovo ThinkSystem SR650 V2 je v garanciji do 31.8.2026
Programska oprema/servisi (vsi strežniki delujejo v virtualnem okolju Vmware Vsphere 7.0 in 8.0)	8x Windows server 2012 R2 ali novejši 2x MS Domain controller (ADC, DNS, DHCP) 1 x Vmware Vsphere ESX 7 2x Veeam, 12.1 backup strežnik SAOR informacijski sistem	

Kritična računalniška strojna oprema in servisi

Seznam kritične strojne opreme:

1x Požarna pregrada Cisco CSF1220CX
1x Požarna pregrada Cisco 5506

Seznam kritičnih servisov:

2x MS 2022 Domain controller (DC, DNS, DHCP)
2x VMWARE strežniška gruča
MS Windows Server 2022 Podatkovni strežnik
Diagnostična avtomatizirana linija BD KIESTRA TLA
Virtualno okolje za SAOR informacijski sistem
2x Veeam Backup

Obseg javnega naročila

Predmet javnega naročila zajema vzdrževanje strojne in sistemske programske opreme Univerze v Ljubljani, Medicinske fakultete, ter zagotavljanje delovanja računalniške infrastrukture v skladu z zahtevami naročnika. Vzdrževanje je razdeljeno v več sklopov:

1. SKLOP 1: Centralna računalniško in komunikacijska infrastruktura UL MF
2. SKLOP 2: Računalniško in komunikacijska infrastruktura Inštituta za patologijo (IP)
3. SKLOP 3: Računalniško in komunikacijska infrastruktura Inštituta za mikrobiologijo in imunologijo (IMI)
4. SKLOP 4: Računalniško in komunikacijska infrastruktura Inštituta za sodno medicino (ISM)

Za sklope 1, 2, 3 in 4 OSNOVNO VZDRŽEVANJE predstavlja operativno vzdrževanje in zajema:

- zagotavljanje razpoložljivosti in zahtevane odzivnosti ter kakovosti izvajanja storitev vzdrževanja strojne in sistemske programske opreme,
- zagotavljanje pravilnega delovanja strojne in sistemske programske opreme,
- zagotavljanje razpoložljivosti in zahtevane odzivnosti ter kakovosti izvajanja storitev vzdrževanja aplikativne programske opreme (podatkovne baze, nadzor in spremljanje delovanja naprav),
- zagotavljanje pravilnega delovanja aplikativne programske opreme (podatkovne baze, nadzor in spremljanje delovanja naprav),
- preventivno vzdrževanje,
- izvajanje postopkov posodobitve vse programske opreme in komponent sistema, ki so potrebni za pravilno in varno delovanje,
- izvajanje postopkov posodobitev in nastavitve opreme za nemoteno delovanje obstoječih sistemskih storitev,
- enkrat letno pregled opreme, priprava poročila in ažuriranje evidenc opreme
- enkrat letno preverjanje gradnikov visoke razpoložljivosti in redundantnih komponent sistema,
- nujni posegi za delovanje sistemske strojne in programske opreme za sistemsko infrastrukturo.
- nastavitve manjšega obsega za ureditev mrežnega prometa na centralnih in končnih točkah omrežja (DNS zapisi, odpiranje vrat, usmerjanje prometa),
- postopki izdelave in zagotavljanje varnostne kopije podatkov in vzpostavitev ponovnega stanja delovanja po izpadu,
- postopki izdelave in zagotavljanje replikacije podatkov na nivoju diskovnega podsistema in vzpostavitev ponovnega stanja delovanja po izpadu (le za Inštitut za Patologijo - velja le za sklop 2)
- analiza možnih izboljšav ali optimizacij rešitev ter izdelava predlogov za optimizacijo za naročnika,
- upravljanje virtualnih strežnikov,
- upravljanje s sistemom data center recovery na nivoju virtualizacije (le za Inštitut za Patologijo- velja le za sklop 2)
- redno administriranje uporabnikov na izbranih aplikacijah (dodajanje, odvzemanje, spreminjanje pravic, …),
- upravljanje fizičnega in logičnega nivoja omrežja,
- upravljanje in zagotavljanje delovanja varnega sistema oddaljenega dostopa do omrežja (VPN koncentratorji),
- upravljanje in zagotavljanje delovanja varnostnih sistemov v omrežju (požarne pregrade) in sistemi za odkrivanje in preprečevanje vdorov,
- upravljanje in zagotavljanje pomožnih servisov za delovanje omrežja (DNS, PROXY, NTP, CA, Monitoring, …),

- reševanje napak pri delovanju v okviru predvidenega odzivnega časa,
- vodenje postopkov prijave, obravnave in odprave okvar pri proizvajalcih opreme v lasti naročnika (Cisco, HPE, Dell in Lenovo, Fortinet),
- sodelovanje z zunanjimi izvajalci pri iskanju možnih vzrokov za težave pri delovanju,
- sodelovanje z zunanjimi izvajalci pri nadgradnji obstoječih rešitev,
- sodelovanje z zunanjimi izvajalci pri vključevanju novih rešitev, sodelovanje in usklajevanje z naročnikom,
- vodenje evidence obsega del iz naslova sodelovanja z zunanjimi izvajalci zaradi vključevanja novih rešitev ali nadgradenj obstoječih rešitev,
- priprava ponudb za dopolnilno vzdrževanje, pomoč uporabnikom (drugi in tretji nivo podpore),
- spremljanje tehnoloških novosti, povezanih z vzdrževano programsko opremo ter priprava predlogov in ukrepov za nemoteno delovanje oz. izboljšanje njenega delovanja,
- objava novih verzij in novonastale dokumentacije, ki so posledica odprave napak in pomanjkljivosti, reševanje problemov ter predlaganje ukrepov za nemoteno delovanje aplikativne programske opreme in optimizacijo delovanja,
- preverjanje delovanja aplikacije na različnih okoljih, ažurno vzdrževanje dokumentacije sistema, redno preverjanje pravilnosti in optimalnosti delovanja sistema,
- intervencije v primeru anomalij, ki jih zazna sam ali jih sporoči naročnik oz. uporabniki,
- učinkovito pomoč in svetovanje ključnim uporabnikom na strani naročnika,
- redno spremljanje delovanja rešitev in poročanje naročniku,
- izdelava rednih in izrednih poročil o delovanju rešitve, ki je predmet vzdrževanja,
- obveščanje naročnika ob zaznanih težavah,
- vodenje evidence obsega del iz naslova sodelovanja z zunanjimi izvajalci zaradi vključevanja novih rešitev ali nadgradenj obstoječih rešitev,
- zagotavljanje in upravljanje sistema za vodenje incidentov in zahtevkov,

Nadzor sistema:

- spremljanje in zbiranje dogodkov iz sistema;
- periodično pregledovanje delovanja sistemske dela podatkovne zbirke;
- stalno spremljanje delovanja podatkovnih virov integriranih na nivoju celotne sistemske infrastrukture in ukrepanje v primeru morebitnih motenj;
- tehnično usklajevanje s posameznimi podatkovnimi viri za zagotovitev operativnega delovanja;
- predlogi ukrepov za preventivno reševanje;

Upravljanje razpoložljivosti, zmogljivosti in kapacitete sistema:

- spremljanje stanja in trendov sistema;
- identificiranje kazalnikov oz. pokazateljev, preko katerih spremljamo, da obratovanje ni ogroženo;
- priprava predlogov in izvajanje ukrepov za zagotovitev zahtevane razpoložljivosti, zmogljivosti (optimizacija) in kapacitete;
- koordinacija izvedbe ukrepov (obveščanje pristojnih oseb), posredovanje dogodka v izvajanje ustreznim izvajalcem.

Upravljanje delovnih postaj – uporabniška podpora

- za 3. sklop mora ponudnik vključiti uporabniško podporo 2x tedensko po 8 ur
- za 4. sklop mora ponudnik vključiti uporabniško podporo 2x tedensko po 4 ure.

Ponudnik mora sistem za upravljanje ter vodenje incidentov in zahtevkov uporabljati Znuny ali ekvivalentno aplikativno rešitev, ki jo UL MF uporablja za vodenje zahtevkov in nudenje pomoči uporabnikov za informacijsko tehnologijo.

Za sklope 1, 2, 3 in 4 DOPOLNILNO VZDRŽEVANJE v dogovoru z naročnikom

Dopolnilno vzdrževanje oziroma nadgradnja informacijske rešitve v dogovoru z naročnikom se izvaja v primeru:

- naknadno definiranih dopolnitev glede na spremembe v uporabniških zahtevah,
- povezave oz. morebitne integracije z različnimi informacijskimi sistemi,
- dodatnih potreb naročnika, ki bi se pokazale med uporabo rešitve.

Dopolnilno vzdrževanje predvidoma zajema:

- sodelovanje pri analizi in pripravi specifikacij uporabniških zahtev za dodajanje novih in izboljšanje obstoječih funkcionalnosti programske opreme,
- dopolnitve komponent rešitev zaradi nadgradnje obstoječih ali vključevanja novih rešitev,
- dopolnitve komponent rešitev zaradi optimizacije delovanja,
- dopolnitev dokumentacije rešitev po izvedenih dopolnitvah,
- izboljšanje obstoječih funkcionalnosti programske opreme,
- izboljševanje lastnosti delovanja, uporabnosti in dograjevanje novih funkcionalnosti ter modulov na podlagi predlogov naročnika, uporabnika ali izvajalca in s strani naročnika potrjenih specifikacij,
- prilagajanje programske opreme glede na spremembe sistemskega okolja in operacijskega sistema v okviru možnosti in zagotovil proizvajalcev oziroma principalov ter glede na potrebe ostalih povezanih informacijskih sistemov,
- prilagajanje in dograjevanje programske opreme glede na vsebinske spremembe,
- priprava analitičnih izdelkov (poročila, statistike),
- odlaganje novih verzij, ki so posledica dopolnilnega vzdrževanja, v repozitorij naročnika,
- pomoč pri odpravi napak na optičnih vodnikih,
- pomoč pri odpravi napak na bakrenih vodnikih in manjše dopolnitve povezav obstoječega ožičenja,
- dokumentiranje novih verzij in funkcionalnosti, ki so rezultat dopolnilnega vzdrževanja, ostale aktivnosti po naročilu naročnika, odprava posledic varnostnih incidentov in pomoč naročniku pri zajezitvi in odpravi varnostnega incidenta; pomoč pri pripravi načrta za odpravo posledic varnostnega incidenta; obveščanje naročnika o morebitnih varnostnih grožnjah na osnovi varnostnih informacij iz svetovnih informacijsko varnostnih virov: pomoč naročniku pri analiziranju škodljive kode; koordinacija in komunikacija z drugimi izvajalci , ki naročniku pomagajo pri odpravi incidenta (npr. UL in Arnes SI-CERT); povrnitev prvotnega stanja iz rezervnih kopij podatkov.

Posebnosti in pogoji za posamezne sklope

Vključitev nove opreme v vzdrževanje

Naročnik si pridržuje pravico, da v času trajanja pogodbe v vzdrževanje vključi dodatno strojno in/ali programsko opremo, ki bo kupljena po sklenitvi pogodbe. Izvajalec se zavezuje, da bo novo opremo vključil v vzdrževanje pod enakimi pogoji, kot veljajo za obstoječo opremo, brez potrebe po sklenitvi aneksa k pogodbi. Nova oprema se lahko vključi v vzdrževanje le, če je po vrsti, kompleksnosti in količini primerljiva z obstoječo opremo ter če skupno povečanje obsega ne presega dogovorjenega praga. V drugih primerih se cena in pogoji uredijo z aneksom oziroma kot dopolnilno vzdrževanje.

Naročnik v okviru tega naročila v vzdrževanje vključuje tudi mrežno opremo, ki je v postopku priklopa in bo nameščena v novi zgradbi Kampusa Vrazov trg 1. Naročnik bo v okviru priklopa zagotovil operativno delovanje ter povezljivost te opreme z obstoječo infrastrukturo Medicinske fakultete.

Seznam mrežne opreme za Centralno računalniško in komunikacijsko infrastrukturo UL MF, ki je v postopku nakupa:

I. OPREMA ZA BREZŽIČNO OMREŽJE (WLAN)	Enota mere	Količina
1.1 Krmilnik za brezžično omrežje		
1.1.1 Virtualni radijski krmilnik, kot npr. Cisco Catalyst 9800-CL	kos	2
1.1.2 5 letna podpora proizvajalca v režimu 8x5xNBD	kpl	2
1.2 Zunanje dostopovne točke		
1.2.1.1 Zunanja dostopovna točka tipa 1 z usmerjenimi antenami, kot npr. Cisco Catalyst CW9163E-E + CW-ANT-D1-NS-00	kos	10
1.2.1.2 5 letna podpora proizvajalca v režimu 8x5xNBD	kpl	10
1.2.2 Zunanja dostopovna točka tipa 2 z vsesmernimi antenami, kot npr. Cisco Catalyst	kos	1

CW9124AXE-E + AIR-ANT2568VG-N= + AIR-PWRINJ7= + AIR-PWR-CORD-CE		
1.2.2.1 5 letna podpora proizvajalca v režimu 8x5xNBD	kpl	1
1.3 Notranje dostopovne točke		
1.3.1 Notranja dostopovna točka tipa 1, kot npr. Cisco Catalyst CW9164I-E	kos	57
1.3.1.1 5 letna podpora ponudnika v režimu 8x5xNBD	kpl	57
1.3.2 Notranja dostopovna točka tipa 1, kot npr. Cisco Catalyst C9115AXI-E	kos	100
1.3.2.1 5 letna podpora ponudnika v režimu 8x5xNBD	kpl	100
II. OPREMA ZA LOKALNO OMREŽJE (LAN)	Enota mere	Količina
2.1 Omrežna oprema		
2.1.1.1 Optično distribucijsko stikalo, kot npr. Cisco Catalyst C9300X-24Y-E	kos	2
2.1.1.2 5 letna podpora proizvajalca v režimu 8x5xNBD	kpl	2
2.1.2.1 Distribucijsko stikalo, kot npr. Cisco Catalyst C9300-48T-E	kos	6
2.1.2.2 5-letna podpora proizvajalca v režimu 8x5xNBD	kpl	6
2.1.3.1 Optično stikalo za priklop multimedije, kot npr. Cisco Catalyst C9300X-12Y-E	kos	3
2.1.3.2 5 letna podpora proizvajalca v režimu 8x5xNBD	kpl	3
2.1.4.1 Optično stikalo za podatkovne centre, kot npr. Cisco Nexus N9K-C93240YC-FX2	kos	4
2.1.4.2 5 letna podpora proizvajalca v režimu 8x5xNBD	kpl	4
2.1.5.1 Dostopovno PoE stikalo, kot npr. Cisco Catalyst C9200-48PXG-E	kos	35
2.1.5.2 5 letna podpora proizvajalca v režimu 8x5xNBD	kpl	35
2.1.6.1 Dostopovno PoE stikalo, kot npr. Cisco Catalyst C9200-48P-E	kos	18
2.1.6.2 5 letna podpora proizvajalca v režimu 8x5xNBD	kpl	18
2.1.7.1 Dostopovno stikalo, kot npr. Cisco Catalyst C9200-48T-E	kos	24
2.1.7.2 5 letna podpora proizvajalca v režimu 8x5xNBD	kpl	24

Strežniška in sistemska oprema (ločen postopek javnega naročila)

Naročnik ločeno pripravlja postopek javnega naročila za nakup strežniške in sistemske opreme, ki bo nameščena v prostorih Kampusa Vrazov trg 1. V okviru tega naročila bo izveden tudi prenos in migracija centralnega dela sistemske infrastrukture na novo opremo.

#	Opis	kos
1	PowerEdge R770 Server - Full Configuration	6
2	Connectrix DS-7710B 8P/24P Switch w/RTF airflow (includes 8x32Gb SFP,ENT Bundle and rack mount kit) [Smart Selection Connectrix DS-7710B|8-24ports|includes 8x32Gb SFP	2
3	Connectrix DS-7710B 8P/24P Switch w/RTF airflow (includes 8x32Gb SFP,ENT Bundle and rack mount kit) [Smart Selection Connectrix DS-7710B|8-24ports|includes 8x32Gb SFP	2
4	Smart Selection PowerStore 1200T_2	2
EXAGRID		
1	Exagrid EX20 (Disk Capacity: Raw 64TB, Useble: 40 TB. 20 TB Full Backup)+10Gigabit Ethernet DualPort SFP+	1

2	Five year 5x8 Customer Support and product Maintenance	1
Vmware		
1	VMware vSphere Foundation 1-Year	288 Core
Veeam		
1	Veeam Data Platform Foundation Socket-Subscription License. - 1 socket. Includes Enterprise Plus Edition features. 5 Years Subscription Upfront Billing & Production (24/7) Support.	12
PAM		
1	Yearly subscription with Gold maintenance - Bastion Core-Resources with unlimited users - resources from 50 -200 for 3 Years	150
2	Yearly subscription with Gold maintenance - AM Named Users, 26 - 50 users for 3 Years	30
CheckMK		
1	Enterprise with Pro support, 3000 services, Virtual appliance and ntopng integration for 1 Year	1

Dodatna oprema in sistemi

Seznam vključuje tudi naslednje rešitve:

- sistem za varnostno kopiranje (ExaGrid),
- virtualizacijsko platformo (VMware),
- rešitev za varnostne kopije (Veeam),
- sistem za upravljanje privilegiranih dostopov (PAM),
- sistem za nadzor (CheckMK).

Naročnik bo v okviru ločenih postopkov nabave zagotovil operativno delovanje in povezljivost nove opreme z obstoječo infrastrukturo Medicinske fakultete.

Naročnik si pridržuje pravico da v času trajanja pogodbe v vzdrževanje vključi dodatno strojno in/ali programsko opremo. Izvajalec se zavezuje, da bo takšno opremo prevzel v vzdrževanje pod enakimi pogoji, kot veljajo za obstoječo opremo, brez potrebe po sklenitvi aneksa k pogodbi.

Skop 1: Centralna računalniško in komunikacijska infrastruktura UL MF

Integracija Microsoft O365 v sistemu UL;

Rezervno opremo priskrbi izvajalec preko garancije ali iz lastne zaloge, če oprema ni v garanciji;

Za vso komunikacijsko opremo iz popisa, za katero proizvajalec ne zagotavlja več podpore oziroma zanjo ni več mogoče skleniti ali podaljšati vzdrževalne pogodbe, mora izvajalec na lastne stroške zagotoviti nadomestno opremo. Nadomestna oprema mora zagotavljati najmanj enakovredne funkcionalnosti, zmogljivosti in razpoložljivost storitev, kot jih je zagotavljala zamenjana oprema.

Za omrežno opremo, ki je v garanciji, se prevzamejo veljavni garancijski pogoji po posameznih kosih opreme, vključno za sistem požarnih pregrad (8×7/NCD);

Za strežniško opremo v garanciji, se prevzamejo veljavni garancijski pogoji po posameznih kosih opreme, vključno za strežnika Lenovo ThinkSystem SR650 (odprava okvare v 6 urah, 6CTR);

Ažurirano evidenco opreme (ključne in ostale), vključno s seznamom opreme na rezervi in sorodne opreme, ki ni predmet pogodbe;

- ažurirano shemo opreme;

Licence:

programska oprema za nadzor delovanja računalniške opreme (licenca WUG poteče maja 2025);
programska oprema za izdelavo rezervnih kopij konfiguracij opreme (licenca KiwiCatTools poteče novembra 2025);
licenca vWLC (garancija in licenca poteče avgusta 2025);

Skop 2: Računalniško in komunikacijska infrastruktura Inštituta za patologijo

Posebnosti in pogoji na Inštitutu za patologijo MF UL za strežniške infrastrukture vključno z DRC (server, networking, security, monitoring):

Ponudnik mora zagotavljati varnost podatkov v skladu z ISO/IEC 27001 in njegovo razširitvijo ISO/IEC 27017

Dokazilo: certifikat ISO/IEC 27001 in ISO/IEC 27017

Podatkovni center mora ustrezati standardu ISO/IEC 27001

Dokazilo: certifikat ISO/IEC 27001

Za DRC:

Ponudnik mora poleg primarnega podatkovnega centra imeti vzpostavljen tudi sekundarni podatkovni center.

Ponudnik mora izpolnjevati naslednje zahteve:

Fizična ločenost podatkovnega centra:
- Sekundarni podatkovni center mora biti fizično ločen od primarnega centra, lociran na drugem seizmološko aktivnem območju, torej na drugi potresni prelomnici ali na območju z drugačnim potresnim tveganjem, z namenom zmanjšanja tveganja zaradi lokalnih okolijskih nesreč (npr. potresi, poplave, požari, izpad elektrike).

Razpoložljivost:
- Primarni in sekundarni podatkovni center morata biti aktivna 24/7.

Povezljivost:
- Ponudnik mora zagotavljati varno in redundantno internetno povezavo med obema centroma.

Varnost data centrov:
- Oba podatkovna centra morata biti varovana z enakovrednimi varnostnimi mehanizmi (fizično varovanje 24/7, voden nadzor dostopa do podatkovnih omar) z vzpostavljenimi sistemi za zaznavo požara.

Varnost podatkov:
- Ponudnik mora zagotavljati varnost podatkov v skladu z ISO/IEC 27001 in njegovo razširitvijo ISO/IEC 27017, za kar mora predložiti certifikacijo in skladnost z obema navedenima certifikatoma.

Varnostno kopiranje:
- Ponudnik mora zagotavljati izvajanje varnostnega kopiranja, obveščanje o uspešnosti izvedbe varnostnega kopiranja in po predhodnem naročilu ter podanem obsegu naročnika periodično izvajati validacijske teste obnovitve varnostno kopiranih podatkov.

Certifikati:
- Oba podatkovna centra morata biti certificirana po standardu ISO/IEC 27001 ter skladna s TIER III ali enakovrednimi zahtevami.

Skop 3: Računalniško in komunikacijska infrastruktura Inštituta za mikrobiologijo in imunologijo

Posebnosti in pogoji na Inštitutu za mikrobiologijo in imunologijo MF UL za operativni management strežniške infrastrukture:

Računalniška oprema za laboratorijsko analizo ni vključena v vzdrževanje javnega naročila.

Administracija Cisco AMP Endpoint protection

Sistemska administracija diagnostične avtomatizirane linije BD KIESTRA TLA

Skop 4: Računalniško in komunikacijska infrastruktura Inštituta za sodno medicino

Integracija s SAOR informacijskim sistemom

Računalniška oprema za laboratorijsko analizo ni vključena v vzdrževanje javnega naročila.

Zahteve v nadaljevanju veljajo za sklop 1, 2, 3 in 4:

Dopolnitve in nadgradnja sistemske infrastrukture

UL MF ima predvidene naslednje dopolnitve in nadgradnje IKT, za katere se bo odločil v dogovoru z naročnikom in glede na potrebe UL MF: Ponudnik je obvezen sodelovati pri uvedbi novih rešitev. Predvidena je uporaba naslednjih rešitev v naslednjih rešitev, ki niso del tega razpisa.

> Vzpostavitev rešitve za nameščanje operacijskega sistema in programske opreme na osebne računalnike

Potrebno je vzpostaviti centralizirano rešitev za pripravo in nameščanje slik (image-ov) operacijskega sistema in osnovne programske opreme na osebne računalnike. Rešitev mora omogočati:

- ustvarjanje in vzdrževanje standardiziranih slik operacijskega sistema s prednameščeno programsko opremo,
- nalaganje teh slik na osebne računalnike prek omrežja (npr. s pomočjo PXE zagona),
- možnost avtomatizirane ali polavtomatizirane namestitve glede na profil uporabnika ali namen računalnika,
- enostavno posodabljanje slik in programske opreme,
- možnost integracije z obstoječim sistemom za upravljanje računalniške opreme.

Cilj je poenostaviti, standardizirati in pospešiti postopek priprave računalnikov za uporabo, obenem pa zagotoviti skladnost z varnostnimi in tehničnimi zahtevami organizacije.

Ureditev varnega tiskanja in digitaliziranja dokumentov z možnostjo overjanja uporabnikov.

Vzpostavitev DRC za UL MF na oddaljeni lokaciji.

Poenotenje nadzora omrežne in strežniške opreme.

Vodenje evidenc in poročanje

Izvajalec je dolžan vzdrževati naročnikovo strojno, programsko opremo in postopke, ki bodo omogočali vodenje, spremljanje in nadzor evidenc prijav napak, varnostnih incidentov, zahtevke za administriranje uporabnikov, ipd. … ter posledično omogočali pripravo verodostojnih poročil.

Izvajalec je dolžan na dnevni ravni ažurno voditi naslednje evidence:

Evidenco incidentov,
Evidenco varnostnih incidentov,
Evidenco zahtev za administriranje sistemskih uporabnikov,
Evidenco aktivnosti na področju kibernetsko varnosti.

V primeru incidentov in varnostnih incidentov je na zahtevo naročnika izvajalec dolžan v najkrajšem razumnem roku pripraviti pisno ali elektronsko poročilo in ga posredovati odgovorni osebi naročnika.

Naročnik zahteva, da za vodenje zahtevkov in poročanja uporablja naročnikovo orodje Znuny. Natančno obliko in dokončno vsebino vseh poročil in evidence bosta naročnik in izvajalec določila v fazi prevzema vzdrževanja IT storitve.

Mesečno poročanje

Mesečna poročila za prejšnji mesec morajo biti priložena pred izstavitvijo računa. Naročnik ima 5 delovnih dni časa za podati morebitne pripombe na priložena poročila. Poročila potrjena s strani naročnika so predpogoj za izstavitev računa.

Vsebina predvidenih mesečnih poročil:

Zbirno poročilo o ugotovljenih in /ali prijavljenih incidentih:

oznaka incidenta, kratek opis incidenta, datum in čas prijave incidenta, prijavitelj incidenta, stopnja in status incidenta,

Zbirno poročilo o varnostnih incidentih:

oznaka varnostnega incidenta, kratek opis varnostnega incidenta, datum in čas prijave varnostnega incidenta, prijavitelj varnostnega incidenta, stopnja varnostnega incidenta, datum in čas začetka odpravljanja varnostnega incidenta, datum in čas odprave varnostnega incidenta, vzrok varnostnega incidenta, ocenjena nastala škoda, kratek opis odpravljanja napake, status na dan zadnji dan v mesecu, predlagani ukrepi za preprečevanje ponovitve varnostnega incidenta.

Zbirno poročilo o Administratorskih zahtevkih:

oznaka zahtevka, kratek opis zahtevka, datum in čas zahtevka, prijavitelj zahtevka, status zahtevka,

Zbirno poročilo o izvedenih preventivnih vzdrževalnih aktivnostih:

datum aktivnosti, kratek opis.

Izvedba rednih pregledov in izdelava poročil

- izvedba letnega pregleda omrežne opreme (meseca marca), vključno s sistemom požarne pregrade, in priprava poročila, ki vsebuje:
- kratek povzetek stanja, zaznanih težav in okvar ter priporočila za izvedbo aktivnosti, vključno s priporočili za nakup nove opreme in opreme za rezervo;
- kratek opis opreme in okolja ter veljavnosti licenc;
- rezultate testiranja delovanja podvojene opreme in rezultate detekcije simuliranih izpadov preko programske opreme za nadzor delovanja računalniške opreme;
- opis razpoložljivih popravkov sistemov ter predlog namestitve;
- opis ključnih opažanj v log datotekah;
- opis zasedenosti virov (diskov, CPU, omrežja) in izdelava predloga za morebitno prerazporejanje bremen;
- opis preverjanja rezervnih kopij nastavitev opreme (preko programske opreme za izdelavo rezervnih kopij konfiguracij opreme); opis preverjanja rezervnih kopij strežnikov za upravljanje požarnih zidov, strežnika vWLC in strežnika za nadzor delovanja računalniške opreme;
- opis skladnosti seznamov opreme v programski opremi za nadzor delovanja računalniške opreme in v programski opremi za rezervne kopije konfiguracij opreme;

- ažurirano evidenco opreme (ključne in ostale), vključno s seznamom opreme na rezervi in sorodne opreme, ki ni predmet pogodbe;
- ažurirano shemo opreme;

Izvedba letnega pregleda strojne strežniške opreme (meseca aprila), vključno s programsko opremo VMWare, in priprava poročila, ki vsebuje:

(enako kot v opisu pregleda omrežne opreme, razen preverjanja rezervnih kopij podatkov);

Izvedba polletnega pregleda okolja Veeam in testno restavriranje podatkov (v začetku junija in decembra) ter priprava poročila, ki vsebuje:

- kratek povzetek stanja, zaznanih težav in okvar ter priporočila;
- kratek opis obravnavane opreme in okolja ter veljavnosti licenc;
- oceno varnosti celotnega sistema (vključno s stanjem MFA in oceno odpornosti glede na znane grožnje) ter priporočila;
- opis razpoložljivih popravkov sistema ter eventualna namestitev;
- pregled delovanja Veeam virtualnega strežnika, vključno s pregledom rezervnih kopij podatkov na vseh uporabljenih medijih, in diagnosticiranje morebitnih težav;
- testiranje obnove podatkov desetih izbranih virtualnih strežnikov iz kopij na diskih, treh iz trakov in treh z oddaljene lokacije;
- preverjanje rezervne kopije strežnika Veeam;
- fizičen izvzem zadnje tedenske, mesečne ali letne kasete iz tračne enote in prenos mesečne ali letne kasete v trezor; ustrezno ažuriranje evidence vstavljenih in izvzetih kaset;
- priprava kaset v tračni enoti za naslednje obdobje;

Izvedba mesečnega pregleda strežnikov Windows in Linux ter priprava poročila, ki vsebuje:

- opis zasedenosti virov sistema in opis pregleda log datotek;
- predlog za namestitev ključnih in drugih popravkov;
- nameščanje popravkov po predhodnem dogovoru z naročnikom (v okviru v tem poglavju navedene kvote ur ali kot dodatne storitve);

Tedenski pregled izvedbe kopij podatkov s programsko opremo Veeam in obveščanje v primeru odstopanja od pričakovanega stanja (ob petkih);

Organiziranje letnega sestanka z naročnikom (maja) s predstavitvijo stanja in predlogi ukrepov.

Zahteve glede razpoložljivosti

Rešitve morajo delovati v režimu 24/7 in biti uporabnikom razpoložljiva vsaj 99,8% (kar predstavlja 17,52 ur nenapovedanega izpada na letni, 86,2 minut na mesečni in 20,2 minut na tedenski ravni).

Zahteve glede odzivnega časa

Incident je definiran kot nedelovanje informacijske rešitve oziroma delovanje, ki ni v skladu z zahtevami, določenimi v specifikaciji rešitve, oziroma tistimi, ki so z izvajalcem naknadno sporazumno dogovorjene oziroma z navodili za uporabo informacijske rešitve. Incidenti se delijo glede na resnost in vpliv na poslovanje, od česar je odvisna tudi hitrost oziroma nujnost odprave.

Odzivni čas je čas, ki preteče od prejema prijave napake, do trenutka, ko izvajalec začne z odpravo napake. Čas odprave napake je čas od trenutka, ko izvajalec začne z odpravo napake, pa do njene odprave (oziroma zagotovitve funkcionalno nadomestne rešitve).

Če izvajalec po pregledu prijave napake ugotovi, da bo za njeno odpravo potrebno več časa, kot je čas odprave napake, ki je podan v preglednici, je dolžan to nemudoma sporočiti naročniku in za vmesni čas vzpostaviti začasno delovanje informacijske rešitve, tako da bo delovni proces uporabnika omogočen.

Odzivni časi, ki jih mora v okviru vzdrževanja ponuditi ponudnik za odpravo napake po prijavi s strani naročnika, uporabnika ali prvega nivoja podpore so prikazani v spodnji tabeli. V kolikor ponudnik v predpisanih odzivnih časih ne vzpostavi funkcionalno stanje informacijskega sistema, se zaračuna

pogodbena kazen v višini, kot je opredeljeno v pogodbi. Za to vrednost se zmanjša znesek mesečnega pavšala za vzdrževanje.

Zahteve glede odzivnega časa pri reševanju zahtevkov

Ponudnik bo pri opravljanju storitev osnovnega vzdrževanja zagotovil reševanje zahtevkov v primeru napak oz. motenj pri delovanju glede na njihovo prioriteto v skladu z odzivnimi časi v spodnji tabeli.

Delovni čas podpore IT na MF je vse dni v letu, ob delavnikih in sobotah od 6. ure do 19. ure, ob nedeljah in praznikih od 8. ure do 16. ure. V primeru, da čas za odpravo napake presega delovni čas, se napaka rešuje tudi izven delovnega časa.

Prioriteta zahtevka	Odzivni čas v delovnem času podpore IT MF	Čas v katerem mora izvajalec odpraviti vzroke napako oz. motnjo*
kritična	1 ura	6 ure
visoka	2 uri	8 ur
pomembna	4 ure	naslednji delovni dan
nizka	1 delovni dan	2 delovna dni

*Velja v primeru menjave mrežne opreme in drugih komponent strojne opreme. V primeru izpada zaradi povrnitve podatkov ali odpravljanja težav, povezanih z varnostnim napadom, mora izvajalec zagotoviti neprekinjeno delo pri odpravi težav, vzpostaviti začasno rešitev ter nato zagotoviti povrnitev sistema v delujoče stanje v najkrajšem možnem času.

Določitev stopnje napake

Napaka (oprema ali storitev)	Vpliv	Opis
Kritična	Zelo visok vpliv	Popolna odpoved delovanja storitev ali poglavitnega dela storitev, ki preprečuje uporabo ključnih delov informacijske rešitve vsem uporabnikom na MF ali uporabnikom na IMI, IP ali ISM
Visoka	Visok vpliv	Delna odpoved delovanja storitev ali poglavitnega dela storitev, ki resno vpliva na uporabo ključnih delov informacijske rešitve skupini uporabnikov.
Pomembna	Srednji vpliv	Oteženo delovanje storitev, ki ne vpliva kritično na uporabo ključnih delov informacijske rešitve pri skupini ali posameznem uporabniku.
Nizka	Nizek vpliv	Katerikoli incident, ki ne vpliva na uporabo ključnih delov informacijske rešitve.

Varnostne zahteve

Zaščita pred zlonamerno kodo in zagotavljanje fizične, organizacijske in informacijske varnosti

Izvajalec mora zagotoviti zaščito vseh aplikacij, ki so, ali bodo vključene v sistemski infrastrukturo UL MF pred zlonamerno kodo. Izvajalec je pri izvajanju opravil in aktivnosti storitev dolžan nenehno uveljavljati najboljše prakse s področij fizične, organizacijske in informacijske varnosti. Izvajalec je dolžan skrbno varovati podatke, s katerimi pride v stik pri izvajanju storitev.

Varnostno kopiranje in povrnitev podatkov

Izvajalec mora zagotavljati avtomatizirano varnostno kopiranje podatkov na opremi naročnika.

Varnostno kopiranje mora:

- zagotavljati varnostno kopiranje različnih virov (datotečni sistem, podatkovne baze, virtualnih strežnikov),
- zagotavljati podporo za polni backup, inkrementalni backup, diferencialni backup, backup baze offline, online, backup log-ov,
- biti (popolnoma) avtomatizirano, tako da omogoča popolno ročno upravljanje, enostavno spreminjanje urnikov arhiviranja, enostavno upravljanje in ustrezno poročanje in obveščanje (elektronska pošta),
- uporabljati sodobne tehnologije za varnostno kopiranje (Disk To Disk, deduplikacija na strojni opremi),
- zagotavljati dolgotrajni iznos varnostnih kopij na trakove.
- zagotavljati samodejno arhiviranje oziroma prenos starejših varnostnih kopij na druga ciljna mesta hrambe,
- zagotavljati podporo hrambe podatkov na object storage nosilcev za hrambo in uporaba »immutable« tehnologije za zaklepanje varnostnih kopij pred izbrisom ali prepisom,
- omogočati mora stiskanje (kompresijo), šifriranje.

Izvajalec mora kvartalno izvesti validacijo varnostnih podatkov in rezultate obnovitve posredovati naročniku.

Omejitev dostopa

Dostop do strežnike infrastrukture je omejen le na potrebne oz. predvidene posege, tako programske kot dostope upravljavskega oz. operativnega osebja. Dostop do podatkov, shranjenih znotraj vseh aplikacij sistemske infrastrukture UL MF, mora biti omogočen in omejen na osnovi pravic dostopa uporabnikov informacijskega sistema. Pravice dostopa so opredeljene za vsako posamezno aplikacijo ali na nivoju posameznih informacijski rešitev UL MF.

Revizijska sled in enotna sinhronizacija časa

Revizijske sledi morajo omogočati rekonstrukcijo in ugotavljanje upravičenosti dostopov do podatkov. Za ta namen je v okviru IT storitve uporabljena enotna sinhronizacija časa.

Varovanje zasebnosti osebnih podatkov

Pri varovanju zasebnosti pacienta in njegovih osebnih podatkov se mora slediti zakonskim zahtevam:

šifriran in digitalno podpisan prenos podatkov izven informacijskega sistema (npr. čezmejna izmenjava,…),
varovanje osebnih podatkov pred nepooblaščenim dostopom.

Postopki ob prevzemu in predaji del

Postopki ob prevzemu del oziroma uvedbi/pričetku izvajanja storitev Izvajalec je dolžan po podpisu pogodbe in pred pričetkom izvajanja storitev v roku, za katerega se dogovori z naročnikom, ki ni daljši od 30 dni od podpisa pogodbe, izvesti naslednje:

- pripraviti opise postopkov po posameznih poglavjih/kategorijah storitev,
- izdelati navodila za svoje kadre za izvajanje del,
- pripraviti kontaktne naslove,
- izvesti interno uvajanje svojih kadrov za izvajanje del na naročnikovih upravljavskih in nadzornih sistemih,
- izvesti preizkus delovanja integracije z naročnikovimi evidencami in informacijskimi sistemi.

Naročnik izvede presojo pripravljalnih del in v primeru, da so skladna s pogoji naročila in pogodbenimi določili naroči/odobri izvajalcu pričetek izvajanja storitev. V nasprotnem zahteva od izvajalca izvedbo

korektivnih ukrepov. Ob pričetku izvajanja storitev naročnik izvajalcu preda vse potrebne podatke in dostopna pooblastila potrebna za izvajanje del. Vsi stroški, ki nastanejo v zvezi s pripravo in prevzemom izvajanja del, bremenijo izvajalca.

Postopki ob predaji del oz. prenosu del na novega izvajalca ter tehnična pomoč in podpora novemu izvajalcu.

V primeru, da bo naročnik objavil novo javno naročilo za izvajanje storitev, ki so predmet te pogodbe, in bo izvajalec, izbran v postopku novega javnega naročila, različen od izvajalca te pogodbe, je izvajalec dolžan v okviru primopredaje poslov nuditi novemu izvajalcu tehnično pomoč in podporo.